

W12D4

BIND SHELL BACKDOOR DETECTION:

Per prima cosa ho aperto kali, usando netcat per connettermi alla porta 1524.

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nc 192.168.50.101 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# netstat -an | grep 192.168.50.100
tcp        0      0 192.168.50.101:1524    192.168.50.100:49542  ESTABLISHED
```

```
File Actions Edit View Help
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open ircs-udp
8009/tcp open ajp13
8180/tcp open unknown
8787/tcp open msgsrvr
39548/tcp open unknown
44504/tcp open unknown
54794/tcp open unknown
57767/tcp open unknown
MAC Address: 08:00:27:EF:D6:EF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 56.32 seconds
```

Una volta trovata la porta (nella quale era già riportata nella scansione con Nessus)

Ho usato il comando: `SUDO NETSTAT -TULNP | GREP` su Metasploitable per trovare quale processo sta ascoltando su quella porta.

IL PID DEL PROCESSO è 4488.

POI CON `SUDO LS -L /PROC/4488/EXE` HO TROVATO LA PATH DEL FILE.

INFINE CON IL COMANDO `SUDO RM -F /USR/SBIN/XINETD` HO RIMOSSO IL FILE COME IN FIGURA.

Alla fine ho fatto `sudo nano /etc/rc.local` per commentare le righe senza gli #

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep :1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4488/xinetd
msfadmin@metasploitable:~$ sudo ls -l /proc/4458/exe
ls: cannot access /proc/4458/exe: No such file or directory
msfadmin@metasploitable:~$ sudo ls -l /proc/4488/exe
lrwxrwxrwx 1 root root 0 2024-07-31 04:21 /proc/4488/exe -> /usr/sbin/xinetd
msfadmin@metasploitable:~$ sudo rm -f /usr/sbin/xinetd
msfadmin@metasploitable:~$
```

NFS EXPORTED SHARE INFORMATION DISCLOSURE

Per rimuovere questa vulnerabilità è stato necessario rimuovere l' asterisco che permetteva l' accesso a qualsiasi host.

```
GNU nano 2.0.7      File: /etc/exports      Modified
# /etc/exports: the access control list for filesystems which may be exported
#                 to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#
/                  192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To
```

```
[ Wrote 12 lines ]
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server restart
* Stopping NFS kernel daemon                                [ OK ]
* Unexporting directories for NFS kernel daemon...          [ OK ]
* Exporting directories for NFS kernel daemon...             [ OK ]
* Starting NFS kernel daemon                                  [ OK ]
```

Alle fine ho lanciato il comando: `sudo /etc/init.d/nfs-kernel-server restart`

VNC SERVER PASSWORD

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ps aux | grep vnc
root      4645  0.0  1.1 13924 12008 ?        S    03:52   0:06 Xtightvnc :0 -d
esktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -r
fbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fo
nts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/shar
e/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co
/etc/X11/rgb
root      4649  0.0  0.1  2724  1192 ?        S    03:52   0:00 /bin/sh /root/.
vnc/xstartup
msfadmin  7940  0.0  0.0  3004   752 tty1      R+   09:58   0:00 grep vnc
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo kill -9 4649
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo kill -9 4645
msfadmin@metasploitable:~$ sudo kill -9 7940
msfadmin@metasploitable:~$ _
```

```
msfadmin@metasploitable:~$ vncserver :1
New 'X' desktop is metasploitable:1
Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log
msfadmin@metasploitable:~$ sudo ls -l ~/.vnc/passwd
-rw----- 1 msfadmin msfadmin 16 2024-07-31 06:26 /home/msfadmin/.vnc/passwd
msfadmin@metasploitable:~$ _
```

Per rimuovere tutte le vulnerabilità ho rimosso tutti i processi con la vecchia password.

In seguito, ho creato una nuova password con il comando vncpasswd, e fatto ripartire il server con il comando vncserver:1

Per avere conferma della password cambiata, ho usato il comando: sudo ls -l ~/.vnc/passwd